AMENDMENTS TO CLAIMS

Claims 1 - 43 (cancelled)

Claim 44 (currently amended): A method for black box analysis of a device capable of accessing protected content, the method comprising:

providing a device to be analyzed;

providing a plurality of group keys comprising n + m group keys, each of n and m being greater than or equal to 1;

inputting to the device a data item comprising encrypted protected content and ~~a plurality of~~ n encrypted versions of a content key for accessing the protected content, each of the ~~plurality of~~ n encrypted versions being encrypted in accordance with a different one of the n ~~a plurality of~~ group keys;

receiving, from the device, decrypted content representing a decryption of the protected content;

~~determining whether the received content is one of the following: erroneous; and null, and producing a result;~~

determining whether the received content is one of the following:

erroneous; and

null,

and producing a result; and

identifying a set of group keys comprising at least one group key which is known to the device based, at least in part, on the result,

wherein the data item also comprises m encrypted versions of at least one invalid content key encrypted in accordance with ~~one of the plurality of group keys~~ the m group keys.

Claim 45 (cancelled)

Claim 46 (original): A method according to claim 44 and also comprising performing the following steps at least once before performing the identifying step:

choosing a new plurality of encrypted versions of the content key; and

performing the inputting, receiving and determining steps.

Claim 47 (original): A method according to claim 46 and wherein the choosing a new plurality step comprises choosing based, at least in part, on at least one of the following:

at least one result of the determining step performed before the choosing step; and

the plurality of encrypted versions of the content key used in the inputting step performed before the choosing step.

Claim 48 (original): A method according to claim 44 and wherein the identifying step comprises identifying the one of the plurality of group keys with which the invalid content key is encrypted.

Claim 49 (original): A method according to claim 44 and wherein the identifying step comprises identifying a group key which is not one of the plurality of group keys with which the invalid content key is encrypted.

Claim 50 (original): A method according to claim 44 and wherein the identifying step comprises identifying a group key which is one of the plurality of group keys with which the invalid content key is encrypted.

Claims 51 - 66 (cancelled)

Claim 67 (new): A method for black box analysis of a device capable of accessing protected content, the method comprising:

providing a device to be analyzed;

analyzing the device, the analyzing comprising:

inputting to the device a data item, the data item comprising:

encrypted protected content;

a plurality of encrypted versions of a content key for accessing the protected content, each of the plurality of encrypted versions being encrypted in accordance with a different one of a plurality of group keys; and

at least one invalid content key encrypted in accordance with at least one additional group key, the additional group key not being comprised in the plurality of group keys;

receiving, from the device, decrypted content representing a decryption of the protected content;

determining whether the received content is one of the following:

erroneous; and

null,

and producing a result; and

identifying a set of group keys comprising at least one group key which is known to the device based, at least in part, on the result.

Claim 68 (new): A method according to claim 67 and also comprising performing the following steps at least once before performing the identifying step:

choosing a new plurality of encrypted versions of the content key; and

performing the inputting, receiving and determining steps.

Claim 69 (new): A method according to claim 68 and wherein the choosing a new plurality step comprises choosing based, at least in part, on at least one of the following:

at least one result of the determining step performed before the choosing step; and

the plurality of encrypted versions of the content key used in the inputting step performed before the choosing step.

Claim 70 (new): A method according to claim 67 and wherein the identifying step comprises identifying the one of the plurality of group keys with which the invalid content key is encrypted.

Claim 71 (new): A method according to claim 67 and wherein the identifying step comprises identifying a group key which is not one of the plurality of group keys with which the invalid content key is encrypted.

Claim 72 (new): A method according to claim 67 and wherein the identifying step comprises identifying a group key which is one of the plurality of group keys with which the invalid content key is encrypted.

Claim 73 (new): A method according to claim 67 and wherein the at least one additional group key comprises a plurality of additional group keys.

Claim 74 (new): A method for black box analysis of a device capable of accessing protected content, the method comprising:

providing a device to be analyzed;

analyzing the device, the analyzing comprising:

providing a plurality of group keys comprising n + m group keys, each of n and m being greater than or equal to 1;

inputting to the device a data item, the data item comprising:

encrypted protected content;

n encrypted versions of a content key for accessing the protected content, each of the n encrypted versions being encrypted in accordance with a different one of the n group keys; and

at least one invalid content key encrypted in accordance with the m group keys;

receiving, from the device, decrypted content representing a decryption of the protected content;

determining whether the received content is one of the following:

erroneous; and

null,

and producing a result; and

identifying a set of group keys comprising at least one group key which is known to the device based, at least in part, on the result.

Claim 75 (new): A method according to claim 74 and also comprising performing the following steps at least once before performing the identifying step:

choosing a new plurality of encrypted versions of the content key; and

performing the inputting, receiving and determining steps.

Claim 76 (new): A method according to claim 75 and wherein the choosing a new plurality step comprises choosing based, at least in part, on at least one of the following:

at least one result of the determining step performed before the choosing step; and

the plurality of encrypted versions of the content key used in the inputting step performed before the choosing step.

Claim 77 (new): A method according to claim 74 and wherein the identifying step comprises identifying the one of the plurality of group keys with which the invalid content key is encrypted.

Claim 78 (new): A method according to claim 74 and wherein the identifying step comprises identifying a group key which is not one of the plurality of group keys with which the invalid content key is encrypted.

Claim 79 (new): A method according to claim 74 and wherein the identifying step comprises identifying a group key which is one of the plurality of group keys with which the invalid content key is encrypted.

Claim 80 (new): A method according to claim 74 and wherein the at least one additional group key comprises a plurality of additional group keys.